UNIVERSITÀ DI PARMA
Dipartimento di Ingegneria e Architettura

# Intrusion Detection Systems

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Course of Cybersecurity, 2022/2023

http://netsec.unipr.it/veltri

# Intrusion Detection System (IDS)

- IDSs are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of intrusions
  - **try to discover attempts to compromise or to bypass the security mechanisms of a computer or network**
  - **generate data as a consequence of normal or abnormal usage**
- IDSs process a stream of events *E1, E2, E3, …,* and past system states *S1, S2, S3,…*, and decide if a new event *E4* in *S4* is the final evidence that an intrusion is occurring
  - **they analyze the manifestation of an attack, not the result of the attack**
- An IDS may try to detect different types of intrusions:
  - **external attackers trying to access a system**
  - **authorized users of the systems who attempt to gain additional privileges for which they are not authorized**
  - **authorized users who misuse the privileges given them**

# Network based IDS

- They detect attacks by capturing and analyzing network packets
  - **monitoring a network segment or switch they can protect multiple host**
- Often consist of a set of single-purpose nodes (called sensors) or hosts placed at various points in a network
  - **sensor can run in “stealth” mode**
- Majority of commercial IDSs
- Advantages:
  - **few placed IDSs can monitor a large network**
  - **little impact upon an existing network**
    - NIDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network
  - **can be made very secure against attack and even made invisible to many attackers**

# Network based IDS

- Disadvantages
  - **may have difficulty in processing all packets in a large or busy network**
    - HW implementation of a NIDS may help
  - **switched networks**
    - networks are subdivided into many small segments (usually one wire per host)
    - most switches do not provide universal monitoring ports
  - **cannot analyze encrypted information**
  - **problems dealing with attacks that fragment packets**
  - **often they cannot tell whether or not an attack was successful**
    - administrators must manually investigate each attacked host to determine whether it was indeed penetrated

# Host based IDS

- Operate on information collected from within an individual computer system
  - **application-based IDSs are actually a subset**
  - **great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system**
- Two types of information sources
  - **operating system audit trails**
    - usually generated at the innermost (kernel) level of the OS
    - more detailed and better protected than application logs
  - **application logs**
    - much smaller than OS trails
    - far easier to comprehend

# Host based IDS

- Advantages
  - **detection of attacks that cannot be seen by a NIDS**
    - e.g. can help detect attacks involving software integrity holes
      - appear as inconsistencies in process execution
  - **they can "see" the outcome of an attempted attack**
    - they can directly access and monitor the data files and system processes usually targeted by attacks
  - **they are unaffected by switched networks and encrypted traffic**
- Disadvantages
  - **harder to manage, as information must be managed for every host monitored**
    - not well suited for detecting surveillance for an entire network
    - the amount of information can be immense
  - **use of the computing resources of the hosts they are monitoring**
  - **the IDS may be attacked and disabled as part of the attack (hosted by the systems it is monitoring)**

# Challenges in Intrusion Detection

- Some challenges:
  - **Detect intrusion in real-time**
    - also in case of a huge stream of events
  - **Integrate different systems so that different analysis techniques and data source are covered**
    - e.g. data provided by network monitors and host auditing facilities
  - **Correlate detection results across different security domains**

# Tools that complement IDS

- Vulnerability Analysis/Assessment Systems
  - **tools to determine whether a network or host is vulnerable to known attacks**
  - **network-based (remote) analysis**
    - testing by exploit
    - inference method (looking for the artifacts that successful attacks would leave behind)
  - **e.g. Nessus, OpenVAS**

- Honeypot System
  - **system that look like a vulnerable system**